IFW

Form PTO-150 (Rev. 7-75) U.S. DEPT. OF COMMERCE PATENT AND TRADEMARK OFFICE

RETENTION LABEL

SERIAL NO.	FILING DATE
10/755,624	01/12/04

ABANDONED FILES: The above application is referred to in application.

Serial No. _____ Filed _____

DO NOT DESTROY

In the United States Patent and Trademark Office (PTO)

$

Serial Number: 10/755,624
Appn. Filed: 1/12/2004
Applicant(s): KEVIN KAWAKITA
Appn. Title: DIGITAL MEDIA DISTRIBUTION CRYPTOGRAPHY USING MEDIA TICKET SMART CARDS
Examiner/GAU: _____

Disclosure Document Reference Letter

Date: 1/3/2004

Assistant Commissioner for Patents
Washington, District of Columbia 20231

Sir:

A disclosure document as identified below was previously filed in the Patent and Trademark Office. As this disclosure relates to the above patent application, applicant(s) request that this Disclosure Document be retained and referenced to the above application.

Disclosure Document Title: DIGITAL MEDIA DISTRIBUTION CRYPTOGRAPHY USING MEDIA TICKET SMART CARDS

Disclosure Document Number: 510,730

Disclosure Document Filing Date: 5/1/2002

Very Respectfully,

Signed Name	N/A Signed Name
KEVIN KAWAKITA Printed Name, First Applicant	Printed Name, Joint Applicant
5812 TEMPLE CITY BL #100 TEMPLE CITY, CA 91780 Address of First Applicant	Address of Joint Applicant

Approved for use through
Patent and Trademark Office, U.S. DE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displa

PTO/SB/95 (08-1999)

Disclosure Document Deposit Request

Mail to:
Box DD
Assistant Commissioner for Patents
Washington, DC 20231

Inventor(s): KEVIN KAWAKITA
Title of Invention: DIGITAL MEDIA DISTRIBUTION CRYPTOGRAPHY USING SMART MEDIA CARDS

Enclosed is a disclosure of the above-titled invention consisting of ~50~ sheets of description and ~3~ sheets of drawings. A check or money order in the amount of ~10~ is enclosed to cover the fee (37 CFR 1.21(c)).

The undersigned, being a named inventor of the disclosed invention, requests that the enclosed papers be accepted under the Disclosure Document Program, and that they be preserved for a period of two years.

Signature of Inventor

5812 TEMPLE CITY BL. #100
Address

KEVIN KAWAKITA
Typed or printed name

4/25/02
Date

TEMPLE CITY, CA 91780
City, State, Zip

NOTICE TO INVENTORS

It should be clearly understood that a Disclosure Document is not a patent application, nor will its receipt date in any way become the effective filing date of a later filed patent application. A Disclosure Document may be relied upon only as evidence of conception of an invention and a patent application should be diligently filed if patent protection is desired.

Your Disclosure Document will be retained for two years after the date it was received by the Patent and Trademark Office (PTO) and will be destroyed thereafter unless it is referred to in a related patent application filed within the two-year period. The Disclosure Document may be referred to by way of a letter of transmittal in a new patent application or by a separate letter filed in a pending application. Unless it is desired to have the PTO retain the Disclosure Document beyond the two-year period, it is not required that it be referred to in the patent application.

The two-year retention period should not be considered to be a "grace period" during which the inventor can wait to file his/her patent application without possible loss of benefits. It must be recognized that in establishing priority of invention an affidavit or testimony referring to a Disclosure Document must usually also establish diligence in completing the invention or in filing the patent application since the filing of the Disclosure Document.

If you are not familiar with what is considered to be "diligence in completing the invention" or "reduction to practice" under the patent law or if you have other questions about patent matters, you are advised to consult with an attorney or agent registered to practice before the PTO. The publication, *Attorneys and Agents Registered to Practice Before the United States Patent and Trademark Office*, is available from the **Superintendent of Documents, Washington, DC 20402.** Patent attorneys and agents are also listed in the telephone directory of most major cities. Also, many large cities have associations of patent attorneys which may be consulted.

You are also reminded that any public use or sale in the United States or publication of your invention anywhere in the world more than one year prior to the filing of a patent application on that invention will prohibit the granting of a patent on it.

Disclosures of inventions which have been understood and witnessed by persons and/or notarized are other examples of evidence which may also be used to establish priority.

There is a nationwide network of Patent and Trademark Depository Libraries (PTDLs), which have collections of patents and patent-related reference materials available to the public, including automated access to PTO databases. Publications such as *General Information Concerning Patents* are available at the PTDLs, as well as the PTO's Web site at www.uspto.gov. To find out the location of the PTDL closest to you, please consult the complete listing of all PTDLs that appears on the PTO's Web site or in every issue of the Official Gazette, or call the PTO's General Information Services at 800-PTO-9199 (800-786-9199) or 703-308-HELP (703-308-4357). To ensure assistance from a PTDL staff member, you may wish to contact a PTDL prior to visiting to learn about its collections, services, and hours.

DESCRIPTION OF INVENTION - List of Reference Numerals

1. smart media card system authority - party S

public key generation authority (PuKGA) - party G
public key distribution authority (PuKDA) - party D
public key escrow authority (PuKEA) - parties En
public key access code authority (PuKAC) - parties EA

48. authorized media distribution authority vendor - party Vn

820. access code toggle field with display

1215. cryptographic digital signal processing chip

1620. cryptographic media player

NOT PART OF INVENTION

800. internet

804. modem

808. smart card reader

812. smart media card

(has embedded tamper resistant non-volatile electrically erasable programmable read-only memory (TNV-EEPROM) also called cryptographic memory and an embedded micro-processor.

816. physical recording medium

(e.g. digital versatile disk read/write (DVD-RW, DVD+RW, DVD-RAM, compact disk record once (CD-R), solid state memory card such as FLASH (R) card, etc.)

820 recording medium drive

824. computer keyboard

828.

832. stereo earphones

836. commercial entertainment store

840. customer party A, B, C, F, ...

848. television broadcast tower

852. television reception antenna

856. digital HDTV broadcast signals

860. digital versatile disk set for commercial movies

864. micro-mirror machine module theater projector

868.

EOF

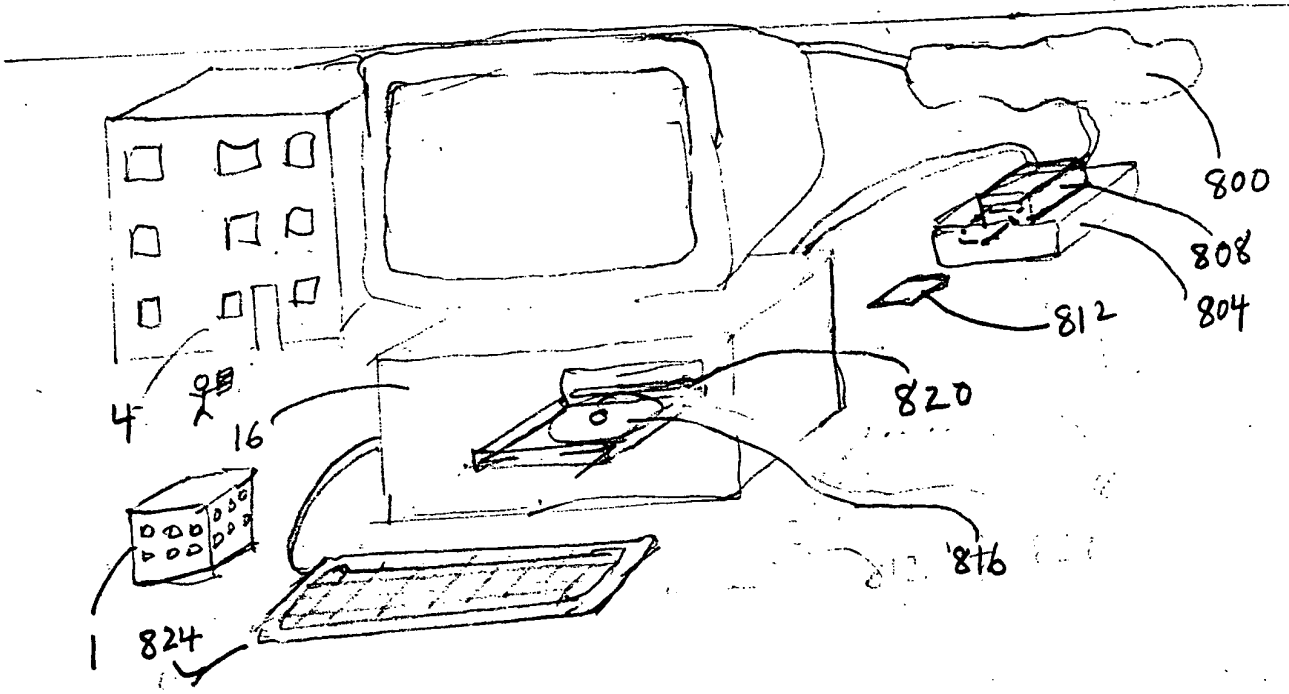

FIG. 1

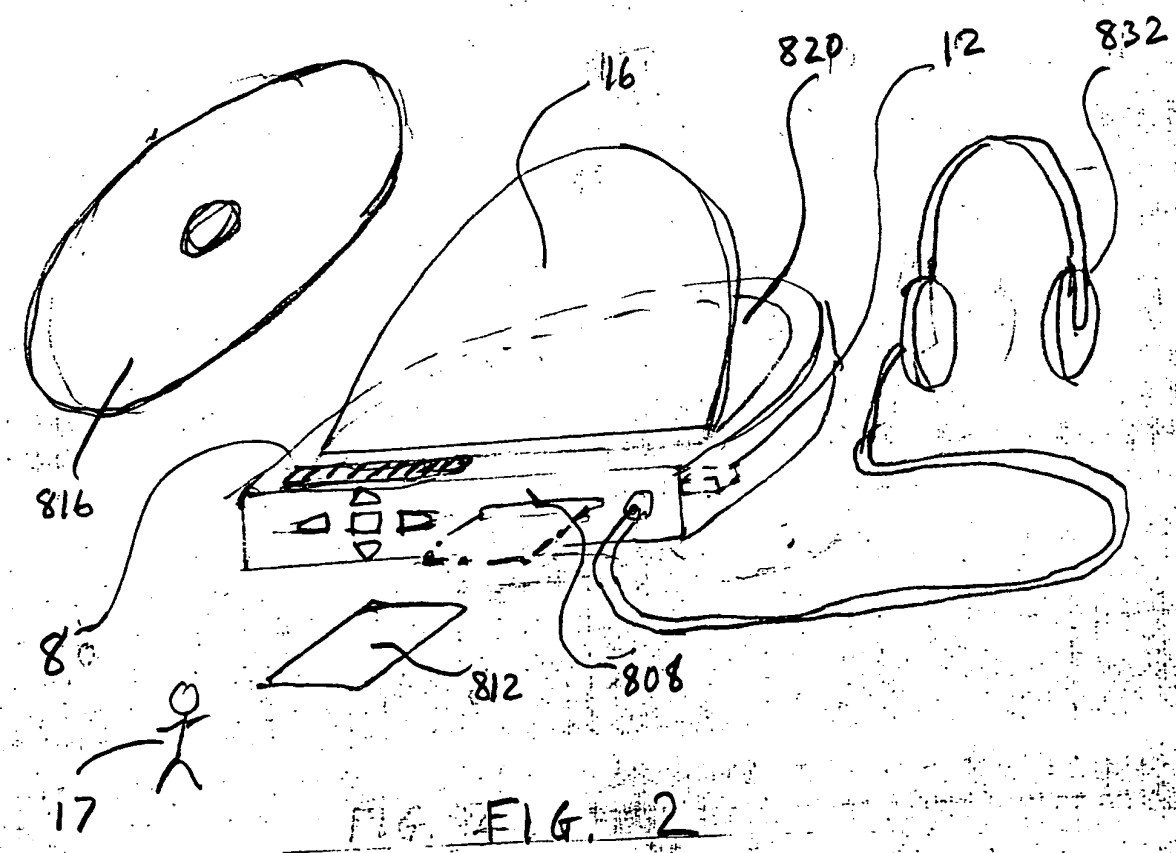

FIG. 2

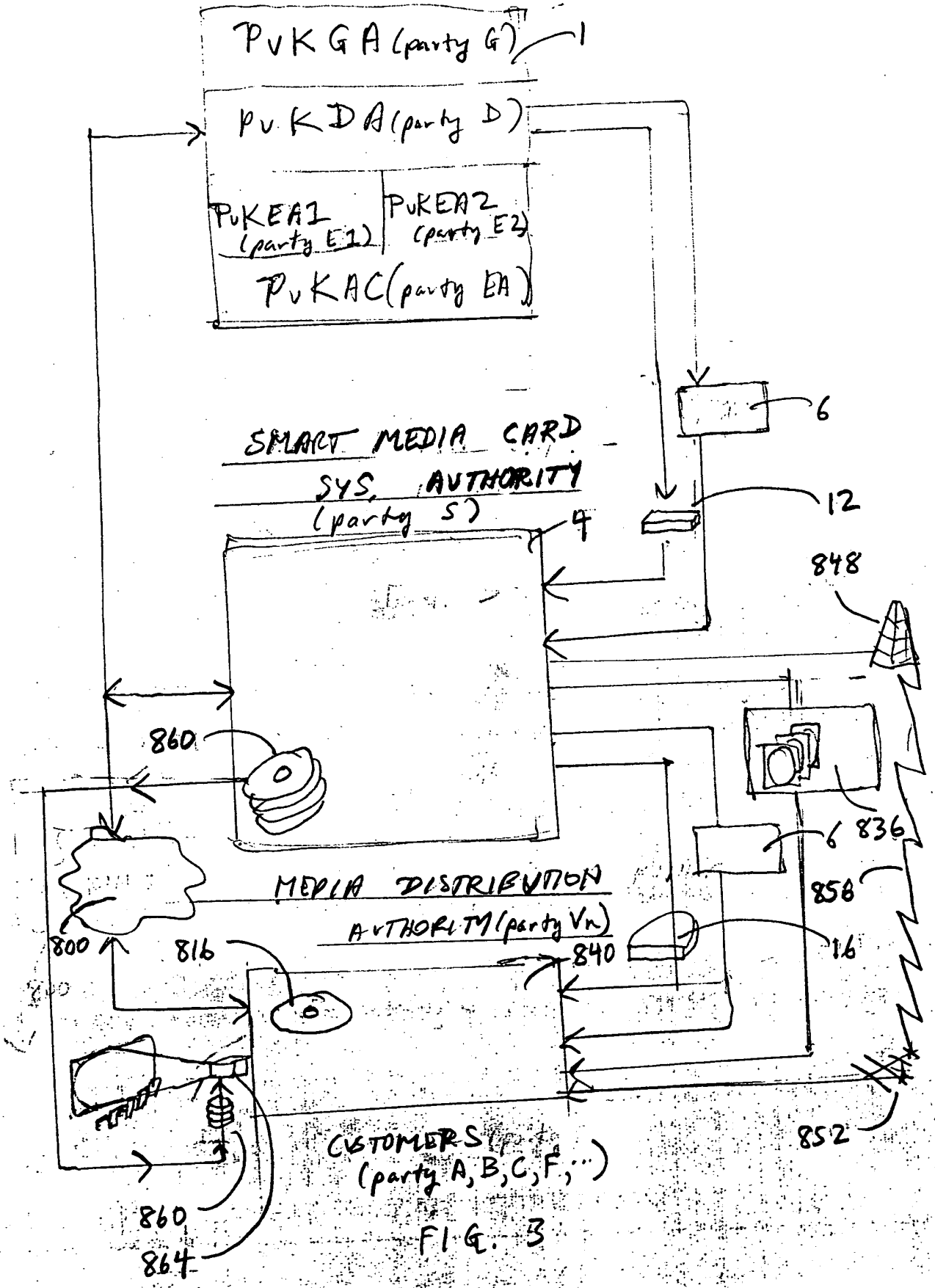
PuKGA (party G)
1
PuKDA (party D)
PuKEA1 (party E1)
PuKEA2 (party E2)
PuKAC (party EA)
6
SMART MEDIA CARD SYS. AUTHORITY (party S)
12
4
848
860
836
6
MEDIA DISTRIBUTION AUTHORITY (party Vn)
858
800
816
840
16
CUSTOMERS (party A, B, C, F, ...)
852
860
864

FIG. 3

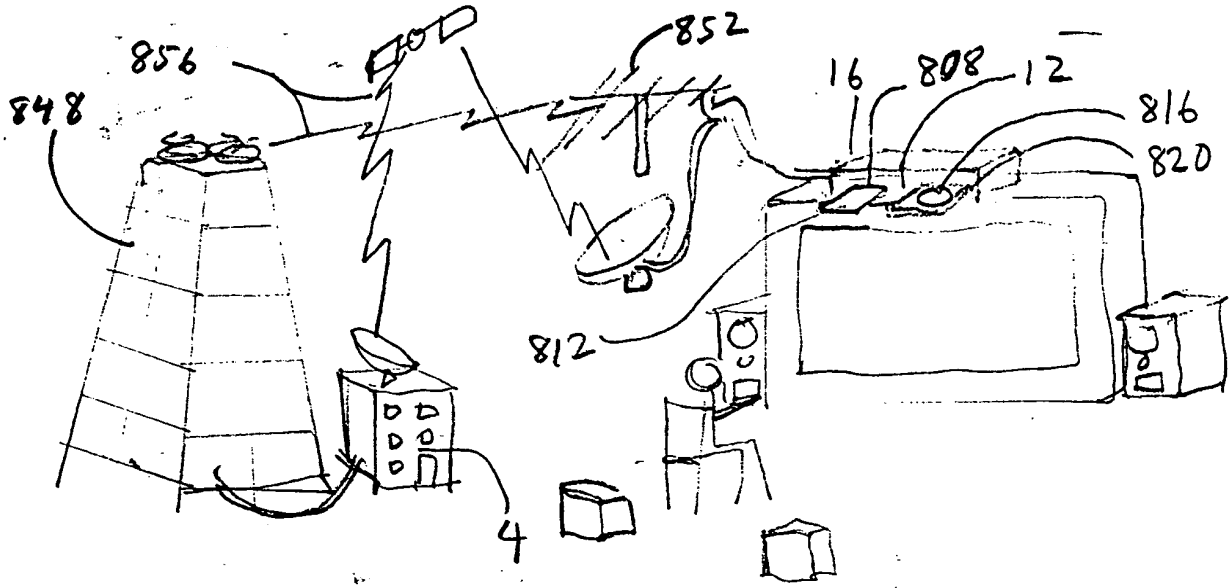

FIG. 4

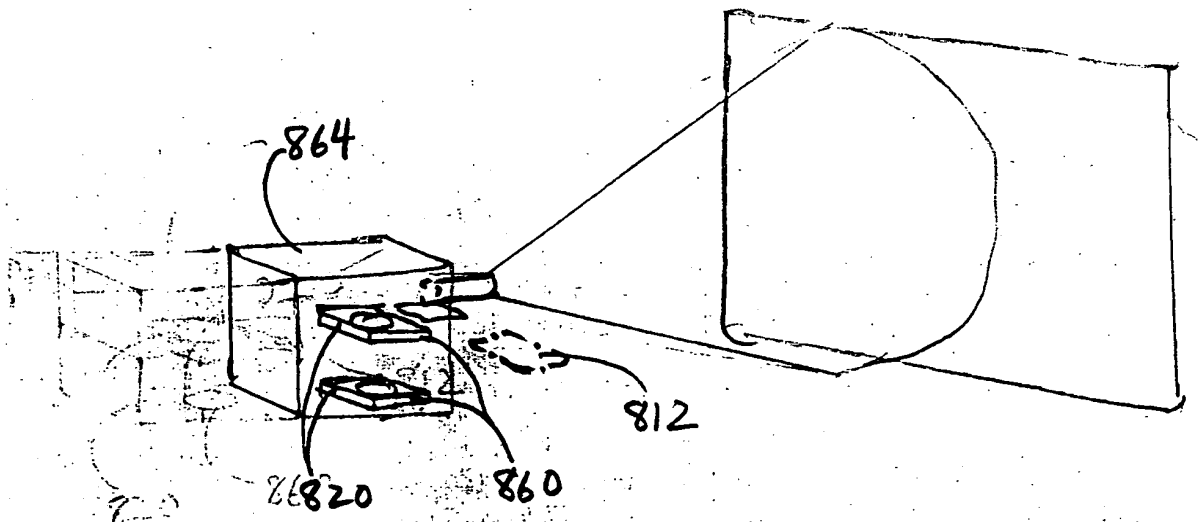

FIG. 5

OBJECTIVES OF DIGITAL MEDIA DISTRIBUTION CRYPTOGRAPHY USING SMART CARDS

OBJECTS & ADVANTAGES - vs. PRIOR ART

A. An object of this invention is to support physical and electronic distribution of custom encrypted digital media limited to digital music, digital movies, digital newspapers, and digital books (not including digital computer programs, digital computer games, and digital computer multi-media)
(see REFERENCES - NON-PATENT LITERATURE [REF 404] - "The Secure Digital Music Initiative (SDMI)").

Napster (R) and Gnutella (R) types of peer to peer web music distribution services of movie picture electronics group (MP3) compressed digital music files allow customers to widely distribute illegal, copyright protected media. The MP3 files are customer created at home personal computers reading non-encrypted music compact disk sources. The music digital master on the compact disks are totally unprotected from illegal copyright piracy.

B. An object of this invention is to use only one smart media card per owner of the corresponding digital media from many different media distribution vendors of digital music, digital movies, electronic newspapers, and electronic books.

One smart media card per music company or one smart media card per item of music will be burdensome and confusing to the customer.

Prior art floppy based or dongle based or keychain based cryptographic key storage was matched one to one with a piece of encrypted data.

C. An object of this invention is to allow the owner's one smart media card to be used with any owner's cryptographic media player [REF 508].

Having one smart media card matched to only the owner's single cryptographic media player [REF 508] will be confusing and limit the choice of players.

D. An object of this invention is to stop the use of any unauthorized digital copying of digital media.

Napster (R) types of peer to peer web music distribution services of movie picture electronics group (MP3) compressed digital music files allow customers to widely distribute illegal, copyright protected media. The MP3 files are customer created at home personal computers reading non-encrypted music compact disk sources. The music digital master on the compact disks are totally unprotected from illegal copyright piracy.

Taiwanese music piracy operations routinely legally copy music cassette tapes, music compact disks, and movie video cassette tapes for overseas distribution into countries not in the international copyright convention. The unencrypted music and movie analog and digital masters are vulnerable and not technologically protected.

E. An object of this invention is to restrict one digital media distribution company's unencrypted digital masters only to itself and absolutely no other party especially prohibiting access by any other competing digital media distribution company.

F. An object of this invention is to allow play counts or count controlled plays or counted decryptions of custom encrypted media including counts of free trial media plays.

Unencrypted digital media can be used an unlimited number of times and allow unlimited perfect copying of digital masters for distribution to unlimited numbers of people.

G. An object of this invention is to provide all public key cryptography functions such as:

1). authentication (like an exchange of photo ID's or thumbprints)

2). encryption/decryption (for privacy)

3). integrity (wholeness or non-tampering)

4). digital signatures (like handwritten signatures)

5). non-repudiation (denying digital signatures)

6). authorization (approval using digital signatures and dating or official post marks)

7). archiving (storing digitally signed documents in a high integrity environment)

8). accessibility (restricting access to authorized users)

9). audit trail (recording accesses to information with Public Key ID's, dates, times, and locations)

10). play counts/play codes for counting paid for and authorized personally encrypted digital media plays and for decrypting them

11). crypto key splitting and key escrow.

12). crypto key administration and key architectures.

Digital media without encryption cannot implement these legal attributes.

H. An object of this invention is to support pass-thru encryption of cryptographic keys called play codes (session keys or 1-time secret keys) and play counts (paid for numbers of plays, -1 for indefinite plays, or counts of free trial plays) for their trip from a media distribution company's central web server over the open internet to a customer's personal computer over wiretappable buses to a secure, cryptographic memory inside of a smart card which is inserted into a smart card reader attached to the same personal computer.

Prior art cryptographic systems have relied upon secure sockets layer (SSL) types of public key distribution. Secure sockets layer does not store cryptographic keys in cryptographic memory. It also does not use pass-thru encryption over wiretappable computer buses. Secure sockets layer is vulnerable to hacker cryptographic algorithm disassembly attacks, logic analyzer attacks, hard disk copying and automated password decryption on hard disk hacker programs, keyboard capture buffers, etc.

I. An object of this invention is to support

physical transfer of encrypted digital media in the form of digital versatile disk read/write, compact disk record once, and FLASH memory cards and also the physical transfer of smart media cards from a customer's personal computer to a cryptographic media player [REF 508] into which both are inserted.

J. An object of this invention is to support pass-thru encryption of cryptographic keys in the form of play codes (session keys or 1-time secret keys) and play counts (paid for numbers of plays, -1 for indefinite plays, or counts of free trial plays) from a smart media card inserted into a smart card reader built-into a cryptographic media player [REF 508] for transferring such keys over wiretappable ("red") computer buses to a cryptographic digital signal processor unit [REF 500], [REF 504] having its own tamper resistant non-volatile electrically erasable programmable read only memory which processor is contained inside of the cryptographic media player [REF 508].

Examples are pass-thru, encrypted, transfer of keys from smart cards to smart card readers (using smart card reader vendor family keys) to cryptographic-DSP's (using cryptographic-DSP vendor family keys).

K. An object of this invention is to support an optional smart media card authentication triangle between the three points of:

point 1, customer A to

point 2, cryptographic media player [REF 508], to

point 3, smart media card A holding a customer, or user's private keys, secret keys, session keys, play codes, and play counts to prevent the use of stolen smart media cards.

Any one of the three points which are detected as unauthorized will stop the smart media card read/write process.

L. An object of this invention is to support a cryptograpic media authentication triangle between the three points of:

point 1, cryptographic media player [REF 508], to

point 2, smart media card holding a
customer, or user's private keys, secret keys, session keys, play codes, and play counts, to

point 3, a copy of 1-way transferred
and custom session key encrypted digital media.

Any one of the three points which are detected as unauthorized will stop the custom encrypted digital media playing process.

M. An object of this invention is to support legal fair use of US copyrighted encrypted digital media or the archiving of two to three copies for personal use. This invention also supports non-copyrighted commercial material and home produced material by allowing unlimited unencrypted plays of the media.

N. An object of this invention is to support legal first use of US copyrighted encrypted digital media or the right of one person to sell or transfer in entirety the encrypted digital media to another person and transfer only relevant smart media card cryptographic keys to the other person's smart media card.

O. An obect of this invention is to support lost and stolen smart media cards.

P. In the 1st alternative embodiment, an object of this invention is to support custom encrypted digital high definition television (HDTV) signals or else cable digital signals for playing upon a cryptographic media player/television/digital recorder with a built-in smart card reader.

Q. In the 2nd alternative embodiment, an object of this invention is to support a high performance, movie cryptographic media player/micro-mirror machine module (MMM) for commercial movie theater use.

...

PROCESS PATENT FOR DIGITAL MEDIA DISTRIBUTION CRYPTOGRAPHY USING SMART CARDS

Definition of trusted ("black") hardware.

Cryptographic keys can only be held in trusted hardware which is equipped with tamper resistant non-volatile electrically erasable programmable read only memory (TNV-EEPROM).

Cryptographic keys even in secret key encrypted form mixed with random noise called "salt" should absolutely never be held in any non-cryptographic memory such as prior art computer hard disks for permanent storage!!!!!!!!!

Non-cryptographic permanent memory examples are ordinary prior art hard disk drives, compact disk record once drives, digital versatile disk read/write drives, or flash (bank programmable) types of solid state memory card drives.

Unencrypted digital masters represent multi-million dollar sources of piracy revenue and are considered a media distribution company's jealously guarded crown jewels. The compromising of cryptographic keys will release multi-million dollar digital masters of hit movies and hit music to the illegal pirate or bootleg video and music industry. Record company promotional pre-releases of music and movie company first release movie masters are routinely copied by illegal copyright pirates even before the first commercial releases to the public!!!!

The media distribution company's secure world wide web server is assumed to be secure and trusted being physically guarded at the media distribution company's central office building and also with internet gateway firewall protection. Web server security levels are from highest to lowest:

1). For highest security, the web server may be an isolated server with no or extremely restricted local area network office connections which holds no unencrypted digital media masters, only encrypted digital media masters. Footprint downloads or data transfer must occur from the ordinary office local area network using hand carried removable hard disk drives and streaming tape cassettes.

2). For next highest security, the web server may be a proxy server or have local area network protocol isolation with the rest of the office. No other office phone line or modem connections should be allowed to avoid points of hacker entry.

The only secure tamper resistant non-volatile electrically erasable programmable read only memory (TNV-EEPROM) or shortened to secure cryptographic memory available in this system is:

1). in the smart media card

2). in the cryptographic media player [REF 508] or more specifically inside of its cryptographic digital signal processor integrated circuit chip (e.g. crypto-MP3 player).

Definition of untrusted ("red") hardware.

The internet is untrusted hardware.

Any non-cryptographic memory is untrusted hardware.

Any non-cryptographic memory devices are untrusted hardware.

Any wiretappable buses are untrusted hardware.

Pass-thru encryption of cryptographic keys using family keys upon unencrypted data always combined with sequence numbers or time stamps if a clock is available upon both sides to prevent recorded replay attacks must be done over all untrusted ("red") hardware and buses.

Any secure sockets layer (SSL) internet connection is considered to be untrusted hardware!!!!!!!

It is definitely not secure enough for transporting cryptographic keys which could be used by pirates to illegally access the clear-text (unencrypted) digital masters of multi-million dollar, commercial digital media such as hit movies, hit music, electronic newspapers, and popular electronic format books. This is because a fully automated hacker personal computer program which can be remotely planted by a virus will automatically extract secure sockets layer private keys and secret keys from hard disks. Such a hacker program will eventually be produced by hackers if indeed it does not already exist because there are no technological barriers to stop the hacker. The hackers will use assembly code dis-assembly and logic analyzers to

reverse engineer the assembly code location and secret key encryption algorithm which mixes the private key and secret key with random noise called "salt" and permanently stores the private key and secret keys on hard disk.
A hacker program will be made to automatically retrieve the secret key encrypted private key and secret keys on hard disk and then randomly try to brute force crack the correct key sequence.

Alternately, a simple keyboard capture buffer remotely planted by a virus can retrieve the keyboard entered customer password and also find out the operating system secret key used to encrypt the private key stored on hard disk for permanent storage.

Factory distribution of cryptographic keys (before any internet based media distribution):

The smart media card system authority, party S, has a division of powers into three components to keep the potential access to plain text digital masters restricted to the originating digital media distribution company (its crown jewels worth multi-millions of dollars):

1). public key generating authority (PuKGA), party G:

has knowledge of whole private keys and whole family keys, but, no knowledge of customer identifications of any kind.

2). public key distribution authority (PuKDA), party D:

has knowlege of customer identifications of the kind registered by customers through retail store forms, web registration, and mail-back postcards, but, no knowledge of whole private keys and whole family keys.

3). public key escrow authorities (PuKEA), parties En (a minimum of parties E1 and E2 for cryptographic keys split into a front-half and a back-half):

party E1 has only half of private keys, half of family keys, half of secret keys.

party E2 has the other halves.

party E1 and party E2 have no customer identification information of any kind.

Central Public Key Generation Authority
(PuKGA) - Party G

The smart media card system authority, party S, has a dedicated function of a public key generation authority, party G,

has knowledge of whole cryptographic keys, but, no knowledge of customer identities or vendor identities!!!!!!

1). Party G generates from true random noise:

the system family key (FaK-F)

which is a family key (common secret key (SeK-F)), FaK-F, where party F is the common family, which is given to the public key distribution authority, party D, for eventual pre-factory distribution to trusted media distribution companies, party Vn.

2). Party G generates an initialization vector (IV) used as a secret key seed (SeK-D) given only to:

a). the public key generation authority (C-PuKGA), party G,

b). the public key distribution authority (C-PuKDA), party D,

The top secret initialization vector (IV) is used as the seed for a message authentication cipher (MAC). A message authentication cipher (MAC) is a message digest cipher (MDC) using a secret seed which restricts its use to classified parties. A message digest cipher (MDC) is a one-way hash code which in example inputs a 512-bit cipher block of data and produces a fixed bit output uniquely representing the data such as a 128-bit pseudorandom output. A message authentication cipher (MAC) code (MAC code) is a fixed bit output such as 128-bits uniquely representing some digital data which only the holders of the initialization vector (IV) can produce.

The initialization vector (IV) is distributed by the party G only to the central public key distribution authority (C-PukDA), party D, who will use it to keep the customer index number (CIN) top secret to stop its use to link cryptographic keys to owners (just as social security numbers should be kept citizen secret). Instead of a

customer index number (CIN), a message authentication cipher code (MAC code) of the customer index number (CIN) is made public called the MAC(CIN).

3). The public key generation authority, party G, pre-factory prepares smart media cards:

The public key generation authority, party G, pre-factory deposits a family key, FaK-F, copy into every blank smart media card before they are given to the public key distribution authority, party D, for eventual physical distribution to trusted media distribution companies, parties Vn, who in turn will factory distribute them to customers at retail stores and in the certified mail.

The party G will generate an incremented customer index number (CIN) which is kept top secret.

The party G will compute a message authentication cipher (MAC) of the customer index number (CIN) called the MAC(CIN) which is used as a public customer identification number.

Party G pre-factory generates public key/private key pairs with the private key always being kept top secret and the public key as public information,

{PuK-A, PrK-A},
{PuK-B, PrK-B,},
etc.

for all customers, party A, party B, etc. and assigns them one by one to customers of unknown identity:

{CIN, MAC(CIN), PrK-A, PuK-A},
{CIN, MAC(CIN), PrK-B, PuK-B},
etc.

Party G pre-factory embeds into smart media card A, the values of:

G-FaK-F
{-----, MAC(CIN), PrK-A, PuK-A}

and into smart media card B, the values of:

G-FaK-F
{-----, MAC(CIN), PrK-B, PuK-B}

etc.

and imprints on the smart card exterior the public customer identification number, MAC(CIN), for identification, since, the central public key distribution authority (C-PuKDA), party D will have no access to the public keys or private keys inside.

Access to the private key field of the smart media cards will be done through an access code (e.g. passcode, passphrase, or password) which initial access code must be denied the Central Public Key Distribution Authority (C-PuKDA), party D, who can have no knowledge of private keys. Therefore, the initial access code is stored inside of a party G database given to a Public Key Access Code Authority (PuKAC) who will later contact the customer with the initial access code:

{
{-----, MAC(CIN), -----, PuK-A,
initial access code},
{-----, MAC(CIN), -----, PuK-B,
initial access code},
etc.
}

Party G gives the smart media cards to the party D who in turn will give them to authorized media distribution companies, parties Vn, for eventual sale to customers.

The party G gives a customer public key database without private keys to the central public key distribution authority (C-PuKDA), party D, for eventual publishing on the world wide web (WWW):

{CIN, MAC(CIN), -----, PuK-A},
{CIN, MAC(CIN), -----, PuK-B},

etc.

The party D will make all public keys without private keys or customer index number (CIN) publicly available over a smart media card system authority internet web server using digital certificate standards (e.g. International Telegraphy Union's (ITU's) X.509 standard).

{---, MAC(CIN), -----, PuK-A,
customer name, etc.},

{---, MAC(CIN), -----, PuK-B,
customer name, etc.},

This new method does not trust other public key systems already in use!!!!!!!!! Existing public key systems such as secure sockets layer (SSL) based public keys are not hacker safe and may be compromised which would give away multi-million dollar in value commercial digital masters for music and movies!!!!!!

The public key generation authority, party G, may destroy the private keys after smart card depositing for absolute privacy. The private keys are kept top secret.

Optionally the party G may use a central public key escrow authority (C-PuKEA), parties En, with a minimum of two escrow parties to hold the front half and the back half of split cryptographic keys, to hold split cryptographic keys.

{---, MAC(CIN), key split PrK-A, PuK-A},
{---, MAC(CIN), key split PrK-B, PuK-B},
etc.

4). The public key generation authority (C-PuKGA), party G, pre-factory prepares the cryptographic digital signal processors for transfer to the public key distribution authority (C-PuKDA), party D, for passing to the media distribution vendors, parties Vn, for eventual manufacturing into cryptographic media players [REF 508] for customer sale.

Party G pre-factory prepares the cryptographic digital signal processing integrated circuits eventually used inside of the cryptographic media players [REF 508] by hardware manufacturers.

Party G must pre-factory install cryptographic keys into the tamper resistant non-volatile electrically erasable programmable read only memory (TNV-EEPROM) of the cryptographic digital signal processing (C-DSP) integrated circuits (IC's).

A cryptographic digital signal processing unit (C-DSP) includes:

cryptographic memory for crypto keys and crypto algorithms,

hardware session key (1-time secret keys) decryption circuits with hardware block error detection and correction,

MPEG X digital decompression circuits,

digital audio/video signal processing circuits,

digital artificial signal degradation circuitry,

analog audio/video or analog signal processing circuits with line amplifiers for output to loudspeakers,

digital video signal modulation to analog for output to computer displays (e.g. SVGA monitors, UXGA monitors, etc.)

Party G installs the smart media card system authority system family key, called party F, FaK-F into the cryptographic digital signal processors (C-DSP's).

Party G generates a top secret vendor index number (VIN) for all media distribution vendors, parties Vn. Party G also generates a public vendor identfication number using a message authentication cipher of vendor index number (MAC(VIN)).

Party G generates vendor private key/public key pairs:

{VIN, MAC(VIN), PrK-Vn, PuK-Vn},
{VIN, MAC(VIN), PrK-Vn, PuK-Vn},
etc.

The whole set of public keys, PuK-Vn, indexed by vendor identification number (MAC(VIN)) will be embedded into each and every cryptographic digital signal processor for eventual use in cryptographic media players:

{---, MAC(VIN), ------, PuK-Vn},
{---, MAC(VIN), ------, PuK-Vn},
etc.

Party G will distribute to the central public key distribution authority (C-PuKDA), party D:

{VIN, MAC(VIN), ------, PuK-Vn},
{VIN, MAC(VIN), ------, PuK-Vn},
etc.

Party D will distribute to each vendor, party Vn, only his own public key data including his own top secret vendor private key, PrK-Vn:

{VIN, MAC(VIN), PrK-Vn, PuK-Vn}

The public key generation authority, party G, may destroy the vendor private keys, PrK-Vn, after cryptographic digital signal processor depositing for absolute privacy. The private keys are kept top secret to each vendor.

Optionally the party G may use a central public key escrow authority (C-PuKEA), parties En, with a minimum of two escrow parties to hold the front half and the back half of split cryptographic keys, to hold split cryptographic keys.

{---, MAC(VIN), key split PrK-Vn, PuK-Vn},
{---, MAC(VIN), key split PrK-Vn, PuK-Vn},
etc.

Party G will also generate unique to each media distribution vendor, party Vn, a unique vendor secret key, SeK-Vn. Party G will give this vendor secret key to the central public key distribution authority for eventual distribution to each media distribution vendor of only his own top secret vendor private key which protects his own digital media masters.

{VIN, MAC(VIN), ------, SeK-Vn},
{VIN, MAC(VIN), ------, SeK-Vn},
etc.

Party G will embed the whole set of unique vendor secret keys, SeK-Vn, indexed by vendor identification number (MAC(VIN)) into each and every cryptographic digital signal processor (C-DSP) for eventual manufacturing into cryptographic media players.

{VIN, MAC(VIN), ------, SeK-Vn},
{VIN, MAC(VIN), ------, SeK-Vn},
etc.

The public key generation authority, party G, may destroy the vendor secret keys, SeK-Vn, after cryptographic digital signal processor depositing for absolute privacy. The private keys are kept top secret.

Optionally the party G may use a central public key escrow authority (C-PuKEA), parties En, with a minimum of two escrow parties to hold the front half and the back half of split cryptographic keys, to hold split cryptographic keys.

{---, MAC(VIN), key split SeK-Vn},
{---, MAC(VIN), key split SeK-Vn},
etc.

Party G gives the programmed cryptographic digital signal processing integrated circuits to the central distribution authority, party D who will pass them to the media distribution vendors, parties Vn, for factory manufacture into cryptographic media players.

5). The public key generation authority (C-PuKGA), party G, may deposit important split cryptographic keys with the central public key escrow authority (C-PuKEA), parties En:

Optionally, the smart media card system authority - public key generation authority function may key split the cryptographic keys as into a front half and a back half and transfer the cryptographic keys to at least two separate public key escrow authorities. The

public key escrow authority function handles the cases of customer lost smart media cards or customer stolen smart media cards or disputes over legal ownership of smart media cards as in divorse cases. This key escrow function allows the smart media card system authority to re-construct cryptographic data and cryptographic keys after lost or stolen smart media cards are reported which might otherwise represent data permanently lost to customers. Disputed legal ownership of smart media cards as in divorse or separation cases may also restore smart media card contents to rightful legal owners even if the smart card itself is not available to a court.

The cryptographic keys should be key split into at least a front half key and a back half key just like breaking it in half. The front half of all keys generated and issued is deposited by the smart media card system authority with a neutral key escrow agent in a computer relational database. The back half of all keys generated and issued is deposited by the smart media card system authority with an entirely separate neutral key escrow agent in a computer relational database.

It is assumed for convenience, payment, and legal ownership that each customer will usually have only one registered smart media card registered with the smart media card system authority for all of his own personal music and movies.

Party E1 receives (front key split halves of):

Customer private key pairs:

(
{---, MAC(CIN), front half PrK-A, PuK-A},
{---, MAC(CIN), front half PrK-B, PuK-B},
etc.
).

Vendor private key, PrK-Vn, pairs:

{
{---, MAC(VIN), front half PrK-Vn},
{---, MAC(VIN), front half PrK-Vn},
etc.
}

Vendor unique secret key, SeK-Vn, pairs:

{
{---, MAC(VIN), front half SeK-Vn},
{---, MAC(VIN), front half SeK-Vn},
etc.
}

Party E2 receives (back key split halves of):

Customer private key pairs:
(
{---, MAC(CIN), back half PrK-A, PuK-A},
{---, MAC(CIN), back half PrK-A, PuK-A},
etc.
}

Vendor private key, PrK-Vn, pairs:

{
{---, MAC(VIN), back half PrK-Vn},
{---, MAC(VIN), back half PrK-Vn},
etc.
}

Vendor unique secret key, SeK-Vn, pairs:

{
{---, MAC(VIN), back half SeK-Vn},
{---, MAC(VIN), back half SeK-Vn},
etc.
}

Central Public Key Distribution Authority
(C-PuKDA) - Party D

The smart media card system authority, party S, has a dedicated function of a central public key distribution authority (C-PuKDA), party D:

which has knowledge of customer identifications and vendor identifications, but, no knowledge of whole cryptographic keys!!!!

1). Input:

Party D receives from the central public key generation authority (C-PuKGA), party G, the following:

Party D receives from party G who generates from true random noise:

the system family key (FaK-F)

which is a common secret keys (SeK-F) where party F is the common family, which is given to the public key distribution authority, party D, for eventual pre-factory distribution to trusted media distribution companies, party Vn.

Party D receives from party G, the initialization vector (IV). Party D will use it to keep the customer index number (CIN) top secret to stop its use to link cryptographic keys to owners (just as social security numbers should be kept citizen secret). Instead of a customer index number (CIN), a message authentication cipher code (MAC code) of the customer index number (CIN) is made public called the MAC(CIN).

Party D will receive from party G a customer public key database without private keys to the central public key distribution authority (C-PuKDA), party D, for eventual publishing on the world wide web (WWW) without the top secret customer index number (CIN):

{CIN, MAC(CIN), -----, PuK-A},
{CIN, MAC(CIN), -----, PuK-B},
etc.

Party D receives from party G the pre-factory programmed smart media cards who in turn will give them to authorized media distribution companies, parties Vn, for eventual sale to customers.

Party D receives from party G media distribution vendor databases:

{VIN, MAC(VIN), ------, PuK-Vn},
{VIN, MAC(VIN), ------, PuK-Vn},
etc.

Party D will distribute to each vendor, party Vn, only his own public key data:

{VIN, MAC(VIN), ------, PuK-Vn}

Party D receives from party G who will also generate unique to each media distribution vendor, party Vn, a unique vendor secret key, SeK-Vn. Party G will give this vendor secret key to the central public key distribution authority for eventual distribution to each media distribution vendor.

{VIN, MAC(VIN), ------, SeK-Vn},
{VIN, MAC(VIN), ------, SeK-Vn},
etc.

Party D receives from party G who will embed the whole set of unique vendor secret keys, SeK-Vn, for every party Vn into each and every cryptographic digital signal processor (C-DSP) for eventual manufacturing into cryptographic media players.

{VIN, MAC(VIN), ------, SeK-Vn},
{VIN, MAC(VIN), ------, SeK-Vn},
etc.

Party D receives from party G the pre-factory programmed cryptographic digital signal processor integrated circuits and party D will in turn distribute the chips to the media distribution companies, parties Vn, for manufacturing into cryptographic media players and for further factory use and eventual customer distribution at retail stores.

2). Party D keeps a top secret computer database record of:

```
{
    authorized media distribution vendor
        index number (top secret) (VIN),
    public vendor identification number =
        message authentication cipher (MAC) of vendor
        index number (MAC(VIN)),
    {---,
    MAC(CIN),
    -----,
    PuK-n,
    eventual registered customer name
        (retail store registered, Web registered, or
        registration postcard, or media distribution vendor
        database updates)
    },
}
```

Party D, look-up of customer name in this top secret database will give the top secret customer index number (CIN). Use of the message authentication cipher (MAC) seeded with the initialization vector (IV) upon the customer index number (CIN) will produce a message authentication cipher code (MAC code) which can be handed to the central public key escrow authorities, parties En, to retrieve key split cryptographic keys and family keys and also used to index the initial smart media card access code database held by the Central Public Key Access Code Authority (C-PuKAC), party EA for mailing or transmitting the initial access code to customers.

3). Party D pre-factory distributes the smart media card system authority system family key, FaK-F, to the media distribution companies, parties Vn.

4). Party D gives the programmed cryptographic digital signal processing (DSP) integrated circuits to the authorized media distribution vendors who will factory manufacture them into cryptographic media players.

Party D keeps a top secret computer database record of:

```
{
    {VIN,
```

MAC(VIN),
------,
PuK-Vn,
------,
vendor identification such as name, address,
etc.
},
}

5). Party D distributes to each media distribution vendor, Vn, his own, unique secret key (SeK-Vn). Party G has already key split these secret keys for deposit with the neutral, key escrow parties, party E1 and party E2.

Party D distributes to each media distribution vendor, Vn, his own, unique vendor private key (PrK-Vn) with a message authentication cipher of vendor identification number (MAC(VIN)). Party G has already key split these secret keys for deposit with the neutral, key escrow parties, party E1 and E2.

Party D distributes to each media distribution vendor, Vn, his plain text vendor identification number which consists of the message authentication cipher of the vendor index number (MAC(VIN)) (for system family key encryption and download with encrypted media to customers to identify the vendor).

6). Party D publishes the customer public key database for use by the media distribution vendors, Vn:

{---, MAC(CIN), -----, PuK-A},
{---, MAC(CIN), -----, PuK-B},
etc.

7). Party D gives to the Central Public Key Access Code Authority (C-PuKAC), Party EA, a top secret computer database record to help in mailing initial access codes to customers of:

{
--------,
public media distribution vendor
identification = message authentication cipher
(MAC) of vendor index number MAC(VIN)),

```
    {---,
    MAC(CIN),
    -----,
    PuK-n,
    eventual registered customer name
        (retail store registered, Web registered, or
        registration postcard)
    },
}
```

Central Public Key Escrow Authorities
(C-PuKEA) - Parties En

The smart media card system authority, party S, has a dedicated function of a central public key escrow authority (C-PuKEA), parties En:

which has knowledge of split cryptographic keys, but, no knowledge of whole cryptographic keys, customer identifications and vendor identifications!!!!

1). Input.

The parties En may optionally receive from the party G (with a minimum of two escrow parties to hold the front half and the back half of split cryptographic keys, to hold split cryptographic keys):

{---, MAC(CIN), key split PrK-A, PuK-A},
{---, MAC(CIN), key split PrK-B, PuK-B},
etc.

The parties En may optionally receive from the party G (with a minimum of two escrow parties to hold the front half and the back half of split cryptographic keys, to hold split cryptographic keys):

{---, MAC(VIN), key split PrK-Vn, PuK-Vn},
{---, MAC(VIN), key split PrK-Vn, PuK-Vn},
etc.

The parties En may optionally receive from the party G (with a minimum of two escrow parties to hold the front half and the back half of split cryptographic keys, to hold split cryptographic keys):

{---, MAC(VIN), key split SeK-Vn},
{---, MAC(VIN), key split SeK-Vn},
etc.

2). An independent function of the smart media card system authority (C-PuKEA), party S, is the central public key escrow authorities, parties En (a minimum of parties E1 and E2),

3). This authority takes care of customer lost, stolen, and legally disputed smart media cards.

Party E1 receives (front key split halves of):

key split smart media card system family key (FaK-F),

key split initialization vector (IV) used as a secret key (SeK) for the message authentication cipher (MAC) used upon the top secret, customer index number (CIN).

(whole message authentication cipher code of customer index number (MAC(CIN)),

key split public key pair n (PuK-n, N),

key split private key pair n (PrK-n, N)).

Party E2 receives (back key split halves of):

key split smart media card system family key (FaK-F),

key split initialization vector (IV) used as a secret key (SeK) for the message authentication cipher (MAC) used upon the top secret, customer index number (CIN).

(public customer identification code =
whole message authentication cipher (MAC) code of customer index number (MAC(CIN)),

key split public key pair n (PuK-n, N),

key split private key pair n (PrK-n, N)).

4). Customer smart media cards which are lost, stolen, or of disputed legal ownership must be handled to preserve use of custom, encrypted digital media still in customer ownership. This is initiated by customers, party A, contacting the central public key distribution authority (C-PuKDA), party D who in turn will contact the parties En using the public customer identification number or MAC(CIN) to retrieve split cryptographic customer keys.

Central Public Key Access Code Authorities
(C-PuKAC) - Parties EAn

The smart media card system authority, party S, has a dedicated function of a central public key access code authority (C-PuKAC), parties EAn:

which has knowledge of smart media card initial access codes and customer identifications in order to mail initial access codes to customers, but, has absolutely no access to smart media cards and no knowledge of whole cryptographic keys!!!!

1). Input.

Party EA receives from the Central Public Key Generation Authority (C-PuKGA), party G, the initial access code database.

```
{
    {-----, MAC(CIN), -----, PuK-A,
        initial access code},
    {-----, MAC(CIN), -----, PuK-B,
        initial access code},
    etc.
}
```

Party EA receives from the Central Public Key Distribution Authority (C-PuKDA), Party D, a top secret computer database record to help in mailing initial access codes to customers of:

```
{
    authorized media distribution vendor id
        (VIN),
    {---,
    public customer identification number
        (MAC(CIN)),
    -----,
    customer n's public key (PuK-n),
    eventual registered customer name
        (retail store registered, Web registered, or
        registration postcard)
    },
}
```

2). The Public Key Access Code Authority (PuKAC), party EA, will later mail in secure certified mail or transmit over Secure Sockets Layer (SSL) to each customer his own initial access code. The initial access code gives customer access to use of his private key field and does not compromise session keys or digital masters.

Authorized Media Distribution Vendors -
Parties Vn

The authorized media distribution vendors, parties Vn:

have no knowledge of whole customer cryptographic keys, but, have knowledge of customer identifications!!!!!

A cryptographic algebra notation implemented in the central media world wide web (WWW) server, party Vn (distribution), for each customer, party A, party B, party C, party E (reserved for key escrow companies), party F (reserved for the common secret family key), party G, party H, etc. is as follows:

1). Input

Party Vn receives from the public key distribution authority (C-PuKDA), party D, pre-factory distributed cryptographic keys:

A). The distribution party, party Vn, the smart media card used by the customer party A (unavailable to the customer himself in secure, tamper resistant, non-volatile, electrically erasabel programmable read only memory (TNV-EEPROM), in short called cryptographic memory) has a pre-factory, party G installed system family key (FaK-F).

The cryptographic media player [REF 508] has a pre-existing, pre-factory, party G installed system family key (FaK-F) in cryptographic memory.

B). The media distribution company, Vn, has a party G, pre-factory distributed unique vendor secret key (SeK-Vn), stored in cryptographic memory.

Any authorized cryptographic media player [REF 508] also receives from party G an entire set of pre-factory distributed unique secret keys, SeK-V1 to Vn for all vendors stored in its cryptographic memory.

C). The media distribution company, Vn, has a party G, pre-factory distributed unique vendor private key (PrK-Vn), stored in cryptographic memory.

Any authorized cryptographic media player [REF 508] also receives from party G an entire set of pre-

factory distributed unique public keys, PuK-V1 to Vn for all vendors stored in its cryptographic memory.

2). The distribution party Vn's computation in his physically secure, media distribution company central office:

These following steps are done in a secure office computer with only a proxy server local area network connection to an internet server (hacker accessible) and also with no phone line access to protect the unencrypted digital masters.

The media distribution party, party Vn, uses his unique message authentication code (MAC) of vendor index number (MAC(VIN)) (the message authentication cipher is not known by the party Vn) as the public vendor identification number (MAC(VIN)) in order to download his public vendor identification number along with an incremented session id number to customers for indexing of the downloaded custom encrypted digital media and also cross-indexing with the encrypted play code with header and encrypted play count with header.

The custom encrypted digital media is defined as:

```
{
vendor identification number MAC(VIN)),
session id number,
play code (SsK-A) encrypted digital media,
}
```

The encrypted play code with header is defined as:

```
{vendor identification number (MAC(VIN)),
session id number,

customer public key (PuK-A) encrypted,
{
vendor secret key (SeK-Vn) encrypted
    {vendor digitally signed (PrK-Vn) play
        code,
    sequence number},
---------,
}
}
```

The play code is defined as the session key (1-time secret key) used to custom encrypt the digital media.

The play count is defined as:

play count = paid for number of plays,
-1 for an infinite count, or
count of free trial plays.

The encrypted play count with header is defined as:

{vendor identification number MAC(VIN)),
session id number,
customer public key (PuK-A) encrypted
{
vendor secret key (SeK-Vn) encrypted
{vendor digitally signed (PrK-Vn) play count,
sequence number},
---------,
}
}

The media distribution vendor, Vn, uses his smart media card system authority issued system family key, FaK-F, to family key pass-thru encrypt the encrypted play count with header, the encrypted play code with header all with sequence numbers to stop recorded replay attacks for download to the customer, party A.

Vn-FaK-F(
(encrypted play count with header)) = V.

The media distribution vendor, party Vn, electronically web bills the customer, party A, over the internet to the prior art customer personal computer A by using credit card numbers transacted over a secure sockets layer (SSL) non-cryptographically secure transaction line.

Sequence numbers - The sequence number is needed to prevent recorded replay attacks on wiretappable buses of pass-thru encrypted signals inside of the cryptographic media player. The sequence number can only be incremented by a party with the vendor secret key (SeK-Vn), customer private key (PrK-n), and system family key (FaK-F) who are the party G for any vendor, the party

Vn only for his own play codes and play counts, or the cryptographic media player, party P, for any vendor which player has a collection of all vendor secret keys (SeK-V1 to Vn) and a collection of all vendor public keys (PuK-V1 to Vn). The cryptographic media player, party P, can also check the vendor digital signature, and can obtain the customer A's private key (PrK-A) and public key (PuK-A) from customer's inserted smart media card A.

The party Vn pass-thru encrypts the play count with header for transfer as:

```
system family key encrypted (Vn-FaK-F):

{vendor identification number MAC(VIN),
session id,
customer public key (PuK-A) encrypted
{
vendor secret key (SeK-Vn) encrypted
    {vendor digitally signed (PrK-Vn) play count,
    sequence number
    },
----------,
}
}= V.
```

which is in cryptographic algebra short-hand notation:

```
Vn-FaK-F
    (
    MAC(VIN),
    session id,
    PuK-A(
    SeK-Vn(
        PrK-Vn(play count), sequence number),
    ))
```

The media distribution vendor, party Vn, uses a true random number generator to create a play code or session key (SsK-A), for customer, party A. The session key is database recorded by party Vn, indexed by the public vendor identification number (MAC(VIN)) along with the digital media title downloaded and date and time.

```
{
vendor identification number (MAC(VIN)),
play code or session key (SsK-A),
```

customer A public key (PrK-A),
digital media title downloaded,
day of distribution,
month of distribution
year of distribution,
time of distribution,
------,
}

The media distribution company, party Vn, digitally signs the play code or session key (Vn-SsK-A), with its own top secret media distribution vendor private key (PrK-Vn), (this is not an encryption step because any holder of the public key (PuK-Vn) can de-scramble the session key):

Vn-PrK-Vn(Vn-SsK-A) = W.

The media distribution company, party Vn, wishes to keep this play code or session key (SsK-A),

top secret from any customers and from any other vendors

which will reveal his multi-million dollar digital masters to digital media competitors.

Party Vn also uses his top secret, unique, secret key (SeK-Vn), to encrypt (1st encryption) the result W and an incremented sequence number to prevent recorded replay hacker attacks. A recorded replay hacker attack is a hacker who wiretaps open computer buses for digital recording and then simply re-introduces the value at a later time without ever decrypting it. Pass-thru encryption of fixed values is vulnerable to recorded replay hacker attacks.

Sequence Number - The sequence number is needed to prevent recorded replay attacks on wiretappable buses of pass-thru encrypted signals inside of the cryptographic media player. The sequence number can only be incremented by a party with the vendor secret key (SeK-Vn), customer private key (PrK-n), and system family key (FaK-F) who are the party G for any vendor, the party Vn only for his own play codes and play counts, or the cryptographic media player, party P, for any vendor which player has a collection of all vendor secret keys (SeK-V1 to Vn) and a collection of all vendor public keys

(PuK-V1 to Vn). The cryptographic media player, party P, can also check the vendor digital signature, and can obtain the customer A's private key (PrK-A) and public key (PuK-A) from customer's inserted smart media card A.

The vendor's own secret key is shared only with the key escrow agents, parties E1 and E2, and a copy kept in the cryptographic media player [REF 508]:

Vn-SeK-Vn(W, sequence number) = X.

The media distribution company, party Vn, can use the play code or unique session key, SsK-A, to uniquely encrypt only party A's digital media masters on the secure office computer before proxy server transfer to a publicly (hacker) accessed internet server or world wide web server.

Vn-SsK-A(digital media)

where:

Vn-SsK-A(data) means party Vn doing session key encryption using party A's play code or session key (1-time secret key) upon digital data.

The following steps can be done by using a proxy server local area network connection to move the encrypted result X and also the uniquely encrypted digital media masters to a world wide web server (with a firewall).

3). 1-way transfer and custom session key encrypted media's unique session key (1-time secret key), SsK-A, used only for customer party A's digital medium:

The following steps can be done by using a proxy server local area network connection to move the encrypted result X and also the uniquely encrypted digital media masters to a world wide web server (with a firewall and anti-viral software updated weekly and run daily).

The media distribution company, party Vn, wishes to restrict this result X uniquely to customer A's smart

media card. Party Vn encrypts (2nd encryption) the result X with the public key of Party A (PuK-A) which only Party A can decrypt with his private key A (PrK-A) stored inside of his smart media card:

Vn-PuK-A(X) = Y.

The media distribution company, party Vn, wishes to restrict result Y to trusted system parties. The media distribution company, party Vn, system family key (common secret key) to pass-thru encrypt (3rd encryption) the result Y with the system family key, FaK, while careful not to pass-thru encrypt the result twice which will undo the pass-thru encryption:

Vn-FaK-F(Y) = Z.

The summation Z of these cryptographic operations becomes the encrypted play code or encrypted session key part of the encrypted play code with header:

encrypted play code with header =

pass-thru encrypted:
{vendor indentification number (MAC(VIN)),
session id,
customer A public key encrypted,
vendor secret key encrypted
{vendor digitally signed play code,
sequence number},
--------,
}

or in cryptographic algebra short-hand notation is:

Vn-FaK-F(
MAC(CIN),
session id,
PuK-A(
Vn-SeK-A
(Vn-PrK-Vn(Vn-SsK-A), sequence no)
))

Sequence numbers - The sequence number is needed to prevent recorded replay attacks on wiretappable buses of pass-thru encrypted signals inside of the cryptographic media player. The

sequence number can only be incremented by a party with the vendor secret key (SeK-Vn), customer private key (PrK-n), and system family key (FaK-F) who are the party G for any vendor, the party Vn only for his own play codes and play counts, or the cryptographic media player, party P, for any vendor which player has a collection of all vendor secret keys (SeK-V1 to Vn) and a collection of all vendor public keys (PuK-V1 to Vn). The cryptographic media player, party P, can also check the vendor digital signature, and can obtain the customer A's private key (PrK-A) and public key (PuK-A) from customer's inserted smart media card A.

where the notation used is:

A-SeK-B(data) means party A doing secret key encryption using party B's secret key upon the clear text data.

SeK means a secret key

FaK means a family key (common secret key)

PuK means a public key

PrK means a private key

SsK means a session key (1-time secret key)

Party F is the family party or set of parties holding the family key (common secret key)

4). Establishment of a media header to help retrieve data from a customer, party A's, smart media card:

{vendor indentification number (MAC(VIN)),
session id number,
encrypted {play count, sequence number},
_____,
}

{vendor indentification number (MAC(VIN)),

session id number,
encrypted {play code, sequence number},
_____,
}

pair to download as an identification header at the start of custom encrypted digital media.

Followed by the custom encrypted digital media of:

{vendor indentification number (MAC(VIN)),
session id number,
play code encrypted digital media,
_____,
}

5). Media distribution vendor, Party Vn, internet world wide web (WWW) download of the encrypted play code with header and encrypted play count with header to the customer A's smart media card A inserted into a smart card reader attached to his personal computer, followed by download of the custom encrypted digital media to the customer A's physical digital media inserted into a drive on his personal computer.

6). Database records for each customer A, party A:

{vendor identification number (MAC(VIN)),
{customer identification of party A such
as name, address, etc.,
MAC(CIN),
PuK-A,
{date/time,
date, month, year,
title of digital media downloaded,
session id number,
play code or session key,
paid for amount,
},
{date/time,
date, month, year,
title of digital media downloaded,
session id number,
play code or session key,
paid for amount,

},
etc.
}

7). Only if a smart media card is directly purchased and registered with the party Vn, a media distribution vendor database of customer identifications must be kept and updates sent to the Central Public Key Distribution Authority (C-PuKDA) who will notify the Central Public Key Access Code Authority (C-PuKAC), party EA, such that party EA can certified mail or securely electronically transmit an initial smart media card access code to the customer.

Customers - Party A

The customers, party n, such as party A, party B, etc. (party D, E, F, G, P, S already in use)

which has knowledge of customer identifications and vendor identifications and his own access code to a particular smart media card for toggle field entry into a cryptographic media player, but, no knowledge of whole cryptographic keys stored in cryptographic memory!!!!

Unique customer A, party A, only once must:

1). Pick up at the retail store a cryptographic media player, a smart media card, and registers the smart media card indirectly with the media distribution vendor or else directly with the Central Public Key Distribution Authority (C-PuKDA), party D, giving his customer name, customer address, etc.

2). Receive from the Central Public Key Access Code Authority (C-PuKAC), party EA, his initial access code to the smart media card which may be changed later.

Unique customer A, party A, upon every custom encrypted digital media download at his prior art world wide web (WWW) connected personal computer:

1). The system family key encrypted vendor indentification number (MAC(VIN)), is downloaded to the customer A's personal computer and to his smart media card (as part of the encrypted play code with header:

play code with header =

{vendor identification number (MAC(VIN)),
session id,
encrypted {play code, sequence number},
)

to ultimately identify the media vendor to the cryptographic media player.

2). This custom encrypted digital media data which is preceeded by a media identification header:

{vendor indentification number (MAC(VIN)),
session id number,
play code encrypted digital media
}

This custom encrypted digital media with media header is internet world wide web downloaded by party Vn to party A's personal computer which transfers the encrypted digital media to a prior art personal computer's prior art peripheral drive containing either digital versatile disk read/write, or compact disk record once, or FLASH memory card. The unique encrypted session key, SsK-A, is transferred through the personal computer smart card reader to an inserted smart media card A.

3). The encrypted physical media and the smart card are transferred by party A to his cryptographic media player [REF 508].

Authorized Cryptographic Media Player -
Party P

The authorized cryptographic media players, party P [REF 508]:

> which have knowledge in cryptographic key memory of the system family key for pass thru encryption, all vendor public keys, and all vendor secret keys, but, no knowledge of customers or cryptographic media!!!!

A cryptographic algebra notation implemented in party A's cryptographic media player [REF 508] having a built-in smart media card reader with party A's smart media card inserted which plays the custom encrpyted digital media using a cryptographic digital signal processor [REF 500], [REF 504] as follows:

1). the custom encrypted physical digital media is installed by customer A in his cryptographic digital media player (e.g. compact disk record once, digital versatile disk read/write, flash bank programmable solid state memory cards, digital cassette tape, etc.).

2). the customer A's own smart media A is installed into the built-in smart media card reader in the cryptographic media player.

3). the cryptographic digital signal processor in the cryptographic media player, party P, retrieves the plain text media header:

> {vendor indentification number (MAC(VIN)), session id, play code encrypted digital media}

> at the start of the media.

4). the cryptographic digital signal processor in the cryptographic media player, party P, does customer triangle authentication to prevent use of lost or stolen smart media cards from:

> point 1, smart media card A,

> point 2, authorized cryptographic media player, party P, and

> point 3, authorized customer A, party A,

from a toggle field entered passcode with a mini-display (e.g. one line liquid crystal display).

Passphrase/passcode entry into a prior art computer keyboard or else a toggle field device with 1-line display such as a liquid crystal display on the cryptographic media player [REF 508].

5). the cryptographic digital signal processor in the cryptographic media player, party P, checks for the correct physical custom encrypted media matched with the correct smart media card by doing media triangle authentication:

point 1, smart media card A with payed for encrypted play codes and encrypted play counts,

point 2, authorized cryptographic media player,

point 3, custom encrypted media A.

6). the cryptographic digital signal processor in the cryptographic media player, party P, retrieves using system family key pass=thru encryption with sequence numbers to avoid recorded replay hacker attacks, the party A's private key, PrK=A, from party A's smart media card A to its own tamper resistant memory. This should be the only private key on the smart media card.

7). the cryptographic digital signal processor in the cryptographic media player, party P, retrieves the encrypted play count with sequence numbers to avoid recorded reaply hacker attacks, from smart media card A, and decrypts it. Where:

play count = paid for number of plays, or
=1 for infinite play, or
count of free trial plays.

If the decrypted play count is greater than one,

play count) > 0 indicates
paid for or free trial plays still remaining

The play count is decremented for accounting purposes, re-encrypted (with an increased sequence number to avoid recorded replay hacker attacks):

```
P-FaK-F(P-SeK-Vn(P-PrK-Vn
   (decremented play count,
   incremented sequence number)))
```

and then sent back to the smart media card A for storage. If the play count is zero, further media plays or custom decryptions are disallowed.

8). the cryptographic digital signal processor in the cryptographic media player, party P, using the

```
{
vendor identification number (MAC(VIN)),
session identification number,
play code encrypted digital media
}
```

identification header from the encrypted digital media, retrieves the encrypted play code with header:

```
{
vendor identification number (MAC(VIN)),
session identification number,
encrypted {play code, sequence number},
}
```

which may be one of many encrypted play codes even from different vendors stored in his smart media card A which is transferred to the cryptographic media player's own tamper resistant memory. The encrypted play code with sequence number is already digitally signed by the media distribution vendor's private key, PrK-Vn, and then 3-way encrypted:

```
Vn-FaK-F(Vn-PuK-A(Vn-SeK-Vn
   (Vn-PrK-Vn(Vn-SsK-A, sequence number)))) =
         encrypted play code or
         encrypted session key
```

NOTE:

Sequence Number - The sequence number is needed to prevent recorded replay attacks on wiretappable buses of pass-thru encrypted signals inside of the

cryptographic media player. The sequence number can only be incremented by a party with the vendor secret key (SeK-Vn), customer private key (PrK-n), and system family key (FaK-F) who are the party G for any vendor, the party Vn only for his own play codes and play counts, or the cryptographic media player, party P, for any vendor which player has a collection of all vendor secret keys (SeK-V1 to Vn) and a collection of all vendor public keys (PuK-V1 to Vn). The player can also check the cryptographic media player, party P, digital signature, and can obtain the customer A's private key (PrK-A) and public key (PuK-A) from customer's inserted smart media card A.

9). The cryptographic digital signal processor inside of the cryptographic media player, party P, having all authorized system vendor public keys, PuK-Vn, and all authorized system vendor secret keys, SeK-Vn, which are pre-factory installed by the public key generation authority, party G, must retrieve only the unique vendor's Vn's public key, PuK-Vn, and secret key, SeK-Vn, using the vendor identification number from step 1) and step 5).

10). The cryptographic digital signal processor inside of the cryptographic media player, party P, uses the system family key (FaK-F), for pass-thru decryption, the customer's private key (PrK-A) obtained from the inserted smart media card A, the vendor Vn's unique secret key (SeK-Vn), to decrypt the digitally signed play code with sequence number, and finally the vendor Vn's unique public key (PuK-Vn) to digitally descramble the play code to give the fully unencrypted play code or session key (1-time secret key):

```
P-SeK-Vn
    (P-PuK-A
    (P-FaK-F
        (encrypted play code with header)
    )) =
    vendor digitally signed play code
        (PrK(play code)),
    sequence number.

P-PuK-Vn(vendor digitally signed play code) =
    play code.
```

NOTE: Sequence Number - The sequence number is needed to prevent recorded replay attacks on wiretappable buses of pass-thru encrypted signals inside of the cryptographic media player. The sequence number can only be incremented by a party with the vendor secret key (SeK-Vn), customer private key (PrK-n), and system family key (FaK-F) who are the party G for any vendor, the party Vn only for his own play codes and play counts, or the cryptographic media player, party P, for any vendor which player has a collection of all vendor secret keys (SeK-V1 to Vn) and a collection of all vendor public keys (PuK-V1 to Vn). The cryptographic media player, party P, can also check the vendor digital signature, and can obtain the customer A's private key (PrK-A) and public key (PuK-A) from customer's inserted smart media card A.

11). The party A's cryptographic digital signal processor, party P, uses the unencrypted play code or session key (D-SsK-A), to decrypt the session key (1-time secret key) encrypted digital medium from party Vn.

12). The party A's cryptographic digital signal procesor will artifically digitally degrade video and audio signals before conversion to analog signals for output to speakers or video displays. This effect will help counter digital recorders wiretapping analog output for music and movie piracy criminal intentions.

A fully digital movie projector using micro-mirror machine (MMM) modules can input encrypted media directly if it has its own decryption digital signal processor function without wiretapping points.

Fully digital loudspeakers can work in a likewise manner with encrypted media.

Customers - Party A

The customers, party n, such as party A, party B, etc. (party D, E, F, G, P, S already in use)

which has knowledge of customer identifications and vendor identifications and his own access code to a particular smart media card for toggle field entry into a cryptographic media player, but, no knowledge of whole cryptographic keys stored in cryptographic memory!!!!

for use in lost, stolen, or legally disputed ownership smart media cards.

1). Must contact the central public key distribution authority (C-PuKDA), party D, with his customer name and public customer identification number (MAC(CIN)) to cancel the old smart media card.

2). Party D will mark the old smart media card as cancelled in his database.

```
{
    authorized media distribution vendor
       identification number (MAC(VIN)),
    {---,
    customer identification number (MAC(CIN)),
    -----,
    customer's public key (PuK-n),

    eventual registered customer name
       (retail store registered,
       Web registered, or
       registration postcard),

    lost/stolen/disputed legal ownership field,
    },
}
```

3). Party D will use the public customer identification number (MAC(CIN)) to contact the central public key escrow authorities, parties En, to obtain the split customer private keys from their databases which are indexed by this number, since, the parties En have absolutely no knowledge of customer identities.

4). Party D will use the public customer identification number (MAC(CIN)) to contact the media distribution vendors, parties Vn, to obtain all the issued encrypted play codes with header (encrypted session keys (SsK-A) also known as 1-time secret keys) and encrypted play counts used by customer A. The encrypted play counts may not be up to date or matching of the encrypted play counts in the lost or stolen smart media card, but, if infinite plays are allowed this is acceptable.

The parties Vn have the database records:

```
{vendor index number (VIN),
vendor identification number (MAC(VIN)),
   {customer identification party A such
      as name, address, etc.
      ---,
      customer identification number (MAC(CIN)),
      public key of customer A (PuK-A),
      {date/time,
      download date,
      download month,
      download year,
      download time,
      title of digital media downloaded,
      session id number,
      paid for amount,
      play code or session key,
      play count,
      },

      {date/time,
      download date,
      download month,
      download year,
      download time,
      title of digital media downloaded,
      session id number,
      paid for amount,
      play code or session key,
      play count,
      },

      etc.
}
```

5). Party D will issue a new smart media card with the previous customer A, private key A, PrK-A, and matching public key A, PuK-A, with the previously issued play codes and play counts. The new smart card will work with existing custom encrypted physical media.

For use in legal transfer of entire ownership of a smart media card A and all custom cryptographic media associated with it from party A to party B. This is called legal "first use."

This is accomplished by use of a cryptographic media player [REF 508] to read from customer party A's smart media card the tamper resistant memory the encrypted 3-way encrypted and digitally signed play code or session key (SsK) with header:

Vn-FaK-F(Vn-PuK-A(Vn-SeK-Vn(
play code with header)
)) =
3-way encrypted and digitally signed play code with header,

NOTE: Sequence Number - The sequence number is needed to prevent recorded replay attacks on wiretappable buses of pass-thru encrypted signals inside of the cryptographic media player. The sequence number can only be incremented by a party with the vendor secret key (SeK-Vn), customer private key (PrK-n), and system family key (FaK-F) who are the party G for any vendor, the party Vn only for his own play codes and play counts, or the cryptographic media player, party P, for any vendor which player has a collection of all vendor secret keys (SeK-V1 to Vn) and a collection of all vendor public keys (PuK-V1 to Vn). The cryptographic media player, party P, can also check the vendor digital signature, and can obtain the customer A's private key (PrK-A) and public key (PuK-A) from customer's inserted smart media card A.

where Vn = the media distribution party
F = family key or group secret key
A-PuK-B = party A using the public key for party B

The cryptographic media player [REF 508], party P, can partially decrypt party A's play codes or session key (SsK-A) in his smart media card A, and re-encrypt it over to party B's play codes or session key (SsK-B),

by the decryption steps:

```
P-SeK-Vn(P-PrK-A(P-FaK-F(
    encrypted play code with header)
    ))
    =
        {
        vendor identification number (MAC(VIN)),
        session identification number,
        vendor digitally signed play code,
        incremented sequence number
        }
    = Y.
```

and then the re-encryption steps:

```
P-FaK-F(P-PrK-B(P-SeK-Vn(Y))) = Z,
```

which changes the private key encryption of customer A to the private key encryption of customer B. The re-encrypted play code with header, Z, can be returned to the smart media card of party B.